CLAIMS

What is claimed is:

1. A booth processor, comprising:

a booth recoder; and

a booth register, wherein an input to the booth register is at least one output from the booth recoder.

2. The booth processor of claim 1, wherein the booth register is a feedback register that stores at least one output value of the booth recoder to be fed back to the boothrecoder.

3. The booth processor of claim 2, wherein the output value is a partial product selection signal, where the partial product selection signal is used to select a partial product value.

4. The booth processor of claim 1, wherein the booth register is a pipeline register, the pipeline register stores output values of the booth recoder.

5. A modulus processor, comprising:

a modulus recoder; and

a modulus feedback register, wherein an input to the feedback register is at least one output from the modulus recoder.

6. The modulus processor of claim 5, wherein the modulus feedback register stores at least one output value of the modulus recoder to be fed back to the modulus recoder.

7. The modulus processor of claim 5, wherein the output value is a multiple modulus selection signal, where the multiple modulus selection signal is used to select a multiple modulus value.

8. A multiplier, comprising:

a booth recoder;

a partial product synch register, wherein an input to the partial product synch register is at least one output from the booth recoder;

a modulus recoder; and

a multiple modulus synch register, wherein an input to the multiple modulus synch register is at least one output from the modulus recoder, where the partial product synch register and the multiple modulus synch register are used to synchronize signals derived from the outputs of the booth recoder and the modulus recoder.

9. The multiplier of claim 8, further comprising:

a booth AND gate, wherein at least one value from the partial product synch register is input to the booth AND gate.

10. The multiplier of claim 8, further comprising:

a modulus AND gate, wherein at least one value from the multiple modulus synch register is input to the modulus AND gate.

11. A multiplier, comprising:

a modulus recoder;

a modulus feedback register, wherein an input to the modulus feedback register is at least one output from the modulus recoder;

a booth recoder; and

a booth register, wherein an input to the booth register is at least one output from the booth recoder, where the modulus feedback register and the booth register save values enabling decreased computation power usage in the multiplier.

12. The multiplier of claim 11, wherein the booth register is a feedback register that stores at least one output value of the booth recoder to be fed back to the booth recoder.

13. The multiplier of claim 12, wherein the output value is a partial product selection signal, where the partial product selection signal is used to select a partial product value.

14. The multiplier of claim 11, wherein the booth register is a pipeline register, the pipeline register stores output values of the booth recoder.

15. The multiplier of claim 11, wherein the modulus feedback register stores at least one output value of the modulus recoder to be fed back to the modulus recoder.

16. The multiplier of claim 15, wherein the output value is a multiple modulus selection signal, where the multiple modulus selection signal is used to select a multiple modulus value.

17. The multiplier of claim 11, further comprising:

a booth AND gate, wherein at least one value from the booth register is input to the booth AND gate.

18. The multiplier of claim 11, further comprising:

a modulus AND gate, wherein at least one value from the modulus feedback register is input to the modulus AND gate.

19. A partial product generator, comprising:

a booth recoder; and

a mux, wherein the mux inputs at least one output from the booth recoder, where the booth recoder and the mux are used to obtain a partial product.

20. The partial product generator of claim 19, further comprising:

a booth AND gate, wherein at least one value from the mux is input to the booth AND gate.

21. The partial product generator of claim 19,

wherein the booth recoder generates a partial product selection signal and a bit pattern is assigned to any value of the partial product selection signal that is prohibited based on a previous value of the partial product selection signal.

22. The partial product generator of claim 21, wherein the bit pattern is chosen so that the hamming distance between the current value of the partial product selection signal and the previous value of the partial product selection signal is reduced.

23. The partial product generator of claim 21, wherein the bit pattern is chosen so that the average temporal hamming distance between the current value of the partial product selection signals and their corresponding previous values are reduced.

24. The partial product generator of claim 21, wherein the booth recoder further comprises:

a first mux, wherein the first mux inputs a first portion of the previous value of the partial product selection signal and outputs a first portion of a current partial product selection signal; and

a second mux, wherein the second mux inputs a second portion of the previous value of the partial product selection signal and outputs a second portion of a current partial product selection signal.

25. The partial product generator of claim 24, wherein the first mux and the second mux are 8:1 muxs.

26. A multiple modulus generator, comprising:

a modulus recoder; and

a mux, wherein the modulus recoder generates a current multiple modulus selection signal unless an enabling signal has a predetermined value, if the enabling signal has a predetermined value, a previous value of the selection signal is used without generating a multiple modulus selection signal, the selection signal is used to select a multiple modulus value.

27. The multiple modulus generator of claim 26, further comprising:

a modulus AND gate, wherein at least one value from the mux is input to the modulus AND gate.

28. The multiple modulus generator of claim 26, wherein the modulus recoder further comprises:

a first mux, wherein the first mux inputs a first portion of the previous value of the selection signal and outputs a first portion of acurrent multiple modulus selection signal; and

a second mux, wherein the second mux inputs a second portion of the previous value of the selection signal and outputs a second portion of acurrent multiple modulus selection signal.

29. The multiple modulus generator of claim 28, wherein the first mux and the second mux are 8:1 muxs.

30. A multiplier, comprising:

a modulus recoder;

a modulus feedback register, wherein an input to the modulus feedback register is at least one output from the modulus recoder;

a modulus synch register, wherein an input to the modulus synch register is at least one output from the modulus recoder;

a booth recoder;

a booth synch register, wherein an input to the booth synch register is at least one output from the booth recoder; and

a booth register, wherein an input to the booth register is at least one output from the booth recoder, where the modulus feedback register and the booth register save values enabling decreased computation power usage in the multiplier, and where the booth synch register and the modulus synch register are used to synchronize signals derived from the outputs of the booth recoder and the modulus recoder to decrease glitches.

31. The multiplier of claim 30, wherein the booth register is a feedback register that stores at least one output value of the booth recoder to be fed back to the booth recoder.

32. The multiplier of claim 31, wherein the output value is a partial product selection signal, where the partial product selection signal is used to select a partial product value.

33. The multiplier of claim 30, wherein the booth register is a pipeline register, the pipeline register stores output values of the booth recoder.

34. The multiplier of claim 30, wherein the modulus feedback register stores at least one output value of the modulus recoder to be fed back to the modulus recoder.

35. The multiplier of claim 34, wherein the output value is a multiple modulus selection signal, where the multiple modulus selection signal is used to select a multiple modulus value.

36. The multiplier of claim 30, further comprising:

a booth AND gate, wherein at least one value from the booth sync register is input to the booth AND gate.

37. The multiplier of claim 30, further comprising:

a modulus AND gate, wherein at least one value from the modulus syncregister is input to the modulus AND gate.

38. The multiplier of claim 30, wherein a multiple modulus value and a partial product value are synchronized by using values from the modulus synch register and values from the booth synch register.

39. A method of increasing computation speed of a radix 2^N Montgomery multiplication, where N>1, comprising:

providing inputs to a booth recoder;

storing outputs of the booth recoder; and

accumulating a result of the Montgomery multiplication,

wherein the storing and the accumulating are performed overlapped in time.

40. The method of claim 39, wherein the outputs of the booth recoder are stored in a pipeline register.

41. A method of reducing power consumption of a radix 2^N Montgomery multiplication, where N≥ 1, comprising:

receiving a modulus, multiplicator, and multiplicand;

synchronizing values related to the modulus, multiplicator, and multiplicand; and

accumulating the values to produce a result of the Montgomery multiplication.

42. The method of claim 41, further comprising:

calculating a multiple modulus using at least one of the modulus, multiplicator, and multiplicand; and calculating a partial product using at least one of the modulus, multiplicator, and multiplicand, wherein the multiple modulus and the partial product are the synchronized values.

43. The method of claim 41, wherein the synchronizing step further comprises:

storing at least two inputs related to the modulus, multiplicator, and multiplicand in synchronization registers.

44. The method of claim 42, further comprising:

matching the arrival time of the partial product and the multiple modulus to an accumulator, reducing overall power consumption of the Montgomery multiplication.

45. A method of reducing power consumption of a radix 2^N Montgomery multiplication, where N>1, comprising:

providing inputs to a booth recoder;

producing a selection signal using the booth recoder;

assigning an inverted bit pattern to any value of the selection signal that is prohibited based on a previous value of the selection signal; and

storing outputs of the booth recoder.

46. The method of claim 45, further comprising:

choosing the inverted bit pattern so that the hamming distance between the current value of the selection signal and the previous value of the selection signal is minimized.

47. The method of claim 45, wherein the bit pattern is chosen so that the average temporal hamming distance between the current values of the selection signals and their corresponding previous values are minimized.

48. A method of reducing power consumption of a radix 2^N Montgomery multiplication, where N≥ 1, comprising:

determining an nth value of an iterative result signal;

providing an enable signal and the nth value of an iterative result signal to a circuit;

if the enable signal renders the (n+1)th value of the iterative result signal meaningless, not calculating the (n+1)th value of the iterative result signal;

feeding back the nth value of the iterative result signal; and

using the nth value of the iterative result signal instead of the (n+1)th value of the iterative result signal.

49. The method of claim 48, wherein the nth and (n+1)th value of the iterative result signal is determined by combinational logic.

50. The method of claim 49, wherein the combinational logic is performed by a MUX.

51. A method of reducing power consumption of a modulus recorder, comprising:

determining an nth value of a multiple modulus selection signal;

storing the nth value of the multiple modulus selection signal in a register;

generating an (n+1)th enable signal, wherein a predetermined value of the enable signal selects a multiple modulus value of zero; and using the nth value of the multiple modulus selection signal without determining the (n+1)th value of the multiple modulus selection signal if the value of the (n+1)th enable signal is the predetermined value.

52. The method of claim 51, further comprising:

selecting the multiple modulus value using the multiple modulus selection signal, wherein the step of selecting is not performed when the enable signal value is the predetermined value.

53. A Montgomery multiplier comprising;

means for inputting, wherein the means for input, enters the values for a modulus, multiplicand, and a multiplier;

means for booth storing, wherein the means for booth storing stores at least one output value from a booth recoder;

means for modulus storing, wherein the means for modulus storing stores at least one output value from a modulus recoder;

means for partial product generation, wherein the means for partial product generation produces a partial product value using the input from the means for input;

means for multiple modulus generation, wherein the means for multiple modulus generation produces a multiple modulus value using the input from the means for input;

means for synchronizing, wherein the means for synchronizing synchronizes the partial product value and the multiple modulus value; and

means for accumulating, wherein the means for accumulating inputs the synchronized partial product value and the multiple modulus value and produces a result for the Montgomery multiplier.